UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/511,466	10/15/2004	Yuji Watanabe	JP920020083US1	2843

877 7590 04/01/2008

IBM CORPORATION, T.J. WATSON RESEARCH CENTER
P.O. BOX 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
04/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/511,466	WATANABE ET AL.	
	Examiner	Art Unit	
	PAUL CALLAHAN	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 October 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1-8-2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-14 are pending and have been examined. This Office Action is directed towards to Applicant's response filed January 8, 2008.

Response to Arguments

2. Applicant's arguments filed January 8, 2008 have been fully considered but they are not persuasive.

The Applicant argues in traverse of the rejections of the claims under 35 USC Sec. 102(e) as anticipated by Matsuzaki. The Applicant asserts that Matsuzaki fails to teach the features of individual key update information corresponding to said specific number of subscriber terminals and used to perform a part of decryption of a second group key, said second group key being updated after a group key is updated. However, the Examiner maintains that these steps are indeed taught at col. 13 line 52 through col. 15 line 45, particularly in col. 15 where common data M2 is shared and decrypted by common data M1 which is dependent on the specific number of terminals and which reads on a group key update.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Matsuzaki et al (US 6,813,357 B1).

Regarding claim 1, Matsuzaki discloses a cryptographic communication system comprising: a key distribution server for distributing a key used to decrypt encrypted information (col. 11, lines 35-47; col. 12, lines45-67; col. 13, lines 1-10); and a specific number of subscriber terminals .using said information (col. 11, lines 35-47; col. 12, lines 45-47), wherein said key distribution server distributes: an encrypted first group key used to decrypt said information (col.13, lines 30-50); individual decryption information corresponding to said specific number of subscriber terminals and used to perform decryption of said first group key (col. 14, lines 1-49); and individual key update information corresponding to said specific number of subscriber terminals and used to perform a part of decryption of a second group key, said second group key being updated after a group key is updated, and wherein said specific number of subscriber terminals decrypt said first group key distributed from said key distribution server by use of results obtained by. processing operations performed based on said key update information previously obtained and used to decrypt said first group key, as well as by use of said decryption information distributed from said key distribution server (col. 15, lines 1-44).

Regarding claim 2, Matsuzaki discloses the cryptographic communication system according to claim 1, wherein said specific number of subscriber terminals implement a part of decryption of said group key, said decryption being performed using said individual key update information, before distribution of said group key (col. 38, lines 1-67; coil 39, lines 1-21).

Regarding claim 3, Matsuzaki discloses the cryptographic communication system according to claim 1, wherein said key distribution server distributes to said specific number of subscriber terminals key update information, used to decrypt said first group key,. together with a third group key, said third group key being in a state before said third group key gets updated to said first group key (col. 31, lines 10-67; col. 32, lines 1-67).

Regarding claim 4, Matsuzaki discloses the cryptographic communication system according to claim 1, wherein in the event where said key distribution server updates said group key, said key distribution server determines which subscriber terminals among said specific number of subscriber terminals are to be excluded and distributes to said specific number of subscriber terminals, together with said group key being updated, said decryption information used by remaining subscriber terminals other than said subscriber terminals to be excluded to make said remaining subscriber terminals able to decrypt said group key being updated (col. 31, lines 10-67; col. 32, lines 1-67).

Regarding claim 5, Matsuzaki discloses a key distribution server for distributing a key used to decrypt encrypted information, comprising: means for generating a first group key used to decrypt said information and encrypting said first group key (col. 32, lines 53:62); means for generating individual decryption information used to perform decryption of said first group key and corresponding to subscriber terminals (col. 32-, lines 63-62; col. 33, lines 1-57); means for generating individual key update information used to perform a part of decryption of a second group key, said second key being updated after a group key is updated, and corresponding to said subscriber terminals (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19); and means for distributing said first group key, said decryption information and said key update information to said subscriber terminals (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1.-19).

Regarding claim 6, Matsuzaki discloses the key distribution server according to claim 5, wherein said means for generating said decryption information determines which terminals among said subscriber terminals are to be excluded and generates said decryption information used by remaining subscriber terminals other than said subscriber terminals to be excluded in order to make said remaining subscriber terminals able to decrypt said group key (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

Regarding claim 7, Matsuzaki discloses a terminal device comprising: means for retrieving from a specific key distribution server a group key encrypted to decrypt encrypted information and decryption information used to decrypt said group key; means for performing a part of decryption of said group key before distribution of said group key; and means for decrypting said group key by use of results obtained by processing operations performed based on a part of decryption of said group key and said decryption information retrieved from said key distribution server (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

Regarding claim 8, Matsuzaki discloses a program for controlling a computer and then distributing a key used to decrypt encrypted information, said program making said computer have capabilities including: a function of generating a first group key used to decrypt said information and encrypting said first group key; a function of generating individual decryption information used to perform decryption of said first group key and corresponding to subscriber terminals; a function of generating individual key update information used to perform a part of decryption of a second group key, said second key being updated after a group key is updated, and corresponding to said subscriber terminals; and a function of distributing said first group key, said decryption information and said key update information to said subscriber terminals via specific communication means (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines. 1-19).

Regarding claim 9, Matsuzaki discloses the program according to claim 8, wherein said function of generating individual decryption information determines which subscriber terminals among said subscriber terminals are to be excluded and generates said decryption information used by remaining subscriber terminals other than said subscriber terminals to be excluded in order to make said remaining subscriber terminals able to decrypt said group key (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

Regarding. claim 10, Matsuzaki discloses a program for controlling a computer and then achieving a specific function, said program making said computer have capabilities including: a function of retrieving from a specific key distribution server a group key encrypted to decrypt encrypted information and decryption information used to decrypt said group key via specific communication means; a function of performing a part of decryption of said group key before distribution of said group key; and a function of decrypting said group key by use of results obtained by processing operations performed based on a part of decryption of said group key and said decryption information retrieved from said key distribution server (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

Regarding claim 11., Matsuzaki discloses a recording medium recording a program thereon for controlling a computer and then distributing a key used to decrypt

encrypted information, said program being made readable by said computer so as to make said computer have capabilities achieved though use of said program, said program including: a function of generating a first group key used to decrypt said information and encrypting said first group key; a function of generating individual decryption information used to perform decryption of said first group key and corresponding to subscriber terminals; a function of generating individual key update information used to perform a part of decryption of a second group key, said second key being updated after a group key is updated, and corresponding to said subscriber terminals; and a function of distributing said first group key, said decryption information and said key update information to said subscriber terminals via specific communication means (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

Regarding claim 12, Matsuzaki discloses a recording medium recording a program thereon for controlling a computer and then achieving a specific function, said program being made readable by said computer so as to make said computer have capabilities achieved though use of said program, said program including: a function of retrieving from a specific key distribution server a group key encrypted to decrypt encrypted information and decryption information used to decrypt said group key via specific communication means; a function of performing a part of decryption of said group key before distribution of said group key; and a function of decrypting said group key by making use of results obtained by processing Operations performed based on a

part of decryption of said group key and said decryption information retrieved from said key distribution server (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

Regarding claim 13, Matsuzaki discloses a key sharing method for making a specific number of terminals share a key used to decrypt encrypted information, said specific number of terminals making use of said information, said method comprising: a step of making said specific number of terminals perform a part of decryption of an encrypted group key used to decrypt said information before distribution of said group key; a step of distributing to said specific number of terminals said group key and individual decryption information used to perform a part of remaining decryption other than said part of decryption of said group key and .corresponding to said specific number of terminals; and a step of making said specific number of terminals perform decryption of said group key using said decryption information being distributed and results obtained by performing a part of decryption of said group key, said part of decryption previously being performed (col. 32, lines 53-62; col. 33, lines 1-67; col. 34, lines 1-19).

Regarding claim 14, Matsuzaki discloses the key sharing method according to claim 13, wherein information used to perform said part of decryption is distributed in advance of distribution of said group key to said specific number of terminals together

with said group key, said group key being in a state before being updated (col. 9, lines 30-62).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Paul Callahan/
March 28, 2008

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137